Appendix 2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	George Alfred Velius	**Group No.:**	2129
Serial No.:	09/886,824	**Atty. Docket No.:**	41942-52970
Filed:	June 21, 2001	**Confirmation No.:**	6850
		Customer No.:	021888
For:	Normalized Detector Scaling	**Examiner:**	Nathan H. Brown, Jr.

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION OF MICHAEL PHILLIPS UNDER 37 C.F.R. § 132

I, MICHAEL PHILLIPS, the below named Declarant, do hereby declare and state as follows:

1. My name is Michael Phillips and I founded and served as Chief Technology Officer for two different advanced speech technology companies (SpeechWorks International - now Nuance Communications, Inc., and Vlingo Corporation).
2. I spent years as a Research Scientist at Carnegie-Mellon University, the Spoken Language Systems Group at the Massachusetts Institute of Technology, and more recently as a Visiting Scientist at MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL).
3. I have extensive experience bringing advanced speech technologies from the laboratory to commercial deployment.
4. In my experience, successful real-world deployments of advanced speech technologies, such as automated speech recognition and speaker identity verification, benefit from tuning of the system through adaptation, which leads to enhanced performance and continuous improvement for users.
5. SpeechWorks International and Nuance Communications, Inc. both had commercially available adaptive speaker identity verification systems that ran on a wide variety of computer hardware and operating systems.
6. **The "adaptive speaker identity verification system" as described in U.S. Patent Application No. 09/886,824 for Normalized Detector Scaling (NDS) utilizes common**

adaptive speaker identity verification systems; the NDS invention, however, provides new adaptive capabilities to provide enhanced verification performance for users of the adaptive speaker identity verification system.

7. **I believe that an individual of ordinary skill in the speech technology art seeing the term "adaptive speaker identity verification system" would clearly understand that this invention involves a commercially-available product (an adaptive speaker identity verification system) and know that a computing platform (including hardware required, such as processors, memory, and machine-readable media) is necessary.**

8. I have read the U.S. Patent Application No. 09/886,824 for Normalized Detector Scaling (NDS) and the claims in question: 23, 25-31, 35, 37-39, 41-44 and 52-59. **I conclude that anyone skilled in the art of deploying an "adaptive speaker identity verification system" would clearly understand this standard industry terminology and would not have to have any additional details regarding the computing platform such as the processors, memory, and machine-readable media. The Invention disclosed in U.S. Patent Application No. 09/886,824 could be readily made by such a person skilled in the art using a common adaptive speaker identity verification system; it is a relatively simple and straightforward process that does not require any undue experimentation.**

9. **The term "adaptive speaker identity verification system" would be well understood and the specification of a particular hardware configuration is not necessary and the invention is not dependent upon a particular hardware or operating system configuration as it can be implemented on the "machine" (computing platform/operating system configuration) on which the adaptive speaker identity verification system runs.**

10. There are abundant commercially-available "adaptive speaker identity verification systems". This includes an adaptive speaker identity verification system that is available from Zehu Technologies (see Exhibit A). Another adaptive speaker identity verification system is available from IBM® (See Exhibit B). Yet another adaptive speaker identity verification system is available from Nuance Communications, Inc. (See Exhibit C). Still another adaptive speaker identity verification system is available from Agnito S.L. (See Exhibit D). Still yet another adaptive speaker identity verification system is available from Loquendo – Vocal Technology and Services (See Exhibit E). Also, another adaptive speaker identity verification system is available from PerSay Ltd (See Exhibit

F). Finally, another adaptive speaker identity verification system is available from SpeechWorks International, Inc. (See Exhibit G). **It is believed that all of these adaptive speaker identity verification systems and the associated computing platform/operating system could be utilized to implement the Applicant's Invention by an individual of ordinary skill in speech application technologies.**

11. I further declare that all statements made herein by my own knowledge are true and all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the above-identified application.

Further Declarant Sayeth Not.

July 13 2009

Date

Michael Phillips

Exhibit A

zehu
technologies

HOME
CONTACT US
NEWSROOM

company

company
technology
products
partners
news/events

ABOUT US   Management   Careers   Contact Us

ABOUT US

Zehu is the premier provider of Adaptive Speaker Verification technologies for integration into simple and enterprise class applications. Our biometric voice authentication technologies enable secured access through speaker verification to improve security beyond traditional authentication methods. The Zehu ASV technology is an integral part of any access control system and increases the threshold of security in identity assurance, fraud protection and security information management.

Zehu's offerings are engineered for cost-effective integration and deployment into multiple applications and usage scenarios. The Zehu software captures incoming data and matches that data against pre-registered voiceprints to provide the highest level of authentication available today. Built on patented architecture, our engineers have created technologies that add value to the systems in which they are integrated. We are dedicated to providing our OEM partners with the comprehensive tools and support required to enhance their applications and platforms.

Originally founded as Cellmax Systems, Zehu began operations in 2005 as a company dedicated to the development of biometric speaker verification technologies. Zehu's headquarters and R&D facilities are based in Tel Aviv, Israel, with offices in New York City.

DANIEL BETTSAK
DIRECTOR GENERAL
MULTITEK CORP.

"Adding Zehu technology to our range of intelligent solutions means added value to our customers, raising their levels of security and controlling access to sensitive customer data at the most reasonable cost. We're looking forward to making this solution commonplace in the Latin American contact center space – the fastest growing in the world, serving both the Spanish and English language commercial and financial markets – as well as the security agencies that protect the Panama Canal region."

HOME | COMPANY | TECHNOLOGY | PRODUCTS | PARTNERS | NEWS/EVENTS | CONTACT US | SITE MAP

PRODUCTS OVERVIEW

Zehu's products are designed as software development kits (SDKS) that provide a package of APIs, libraries and tools to OEM applications.

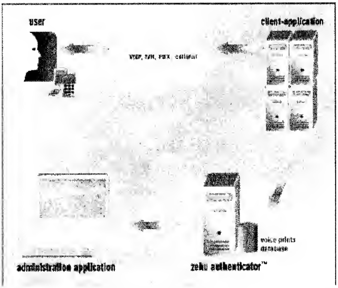
ZEHU AUTHENTICATOR ™

Zehu Authenticator ™ is a biometric verification platform that uses a voice biometric technology for real time verification of a person's identity. By matching the user's voice to a mathematical voice model stored in a database, Zehu Authenticator ™ returns a highly accurate authentication within seconds. This is performed using one of the following three possible authentication methods:

* Fixed Sentence: a predefined sentence used to enroll and authenticate users
* Flexible Sentence: a user-selected phrase for registration and authentication
* Free Speech: users speak freely during registration and authentication

Architecture

Zehu Authenticator ™ consists of a voice verification server, a database that stores mathematical voice models, system setting and configuration, and a web-based management application, as shown in the following system architecture.



The system can be easily integrated with many applications such as IVR platforms, time and attendance systems, smart card technologies, as well as other biometric platforms.

JODY BOUVIER
VOIP/NETWORK
ADMINISTRATOR
EDISON CHOUEST
OFFSHORE

"We have been working with Zehu on our Teledata Technology T3 voice mail servers since October 2006... Zehu provides complete ease of use. For example, when calling my voice mailbox from a cell phone, I simply say my verification sentence and listen to my messages. There's none of the distraction of having a key in a pass-code. More importantly, the level of accuracy for speaker verification is extraordinarily high – even over low quality landlines or compressed and distorted cell phone networks...I highly recommend Zehu."

Exhibit B

Speaker Identity Verification Extensions
for WebSphere Voice Server
Enhancing Security for Telephone based Interactions

IBM

Using voiceprints to verify a user with speaker verification

When it comes to providing secure access for self-service, telephone-based applications, most solutions are prone to fraud, as the authentication mechanism is based on information that is easily compromised.

What is Speaker Identity Verification Technology?

"Speaker Identity Verification technology enables a non-intrusive and highly accurate mechanism for authenticating users based on the analysis of their voice. Speaker Identity Verification technology provides much more accurate and secure speech applications. Speaker verification is the ability to authenticate someone's identity based on their voice. It significantly reduces the risks of unauthorized access, since the authentication mechanism uses the unique features of someone's voiceprint."

A New Way to Authenticate in a VoiceXML Application

The addition of speaker identity verification provides a VoiceXML application with a new means for authentication - using voice.

IBM's speaker *identity* verification is an optional component of the WebSphere Voice Server. Speaker *identity* verification enables a telephone-based self-service application (running on any Web application server) to accept speech and match it against an enrolled voiceprint for caller authentication.

WebSphere Voice Server speaker identity verification is completely developed in Java, and leverages the highly scalable and robust WebSphere Application Server's Java 2 Enterprise Edition (J2EE) services. It brings all the WebSphere Application Server benefits to speaker verification, including:

- reduced deployment costs with integration into the IT infrastructure;
- central and common management;
- advanced system monitoring;
- increased reliability;
- simplified problem determination.

Identity theft is the number one crime in America today. Speaker *identity* verification instills confidence in customers in regards to the security of their data. The ability to use one's voice for authentication adds an extra layer of protection to sensitive information.

For example, if a user's account ID and password are stolen, the imposter will be detected by the system when he tries to access account specific information while pretending to be someone else. The use of voiceprints increases the reliability of identity verification and makes it much more difficult for someone to break into a user's account.

IBM's Speaker Verification Technology

The technology behind the speaker identity verification feature of WebSphere Voice Server provides customers with a competitive edge.

IBM's Speaker *Identity* Verification technology provides a grammar, language, and text independent authentication mechanism. You can enroll saying anything, in any language, and have it verify you, saying anything, in any language! Some of the benefits of the speaker *identity* verification feature of WebSphere Voice Server include:

- Language Independence
  - One speaker verification engine can handle all languages;
  - Speaker can enroll in one language and be verified in another.
- Text Independence
  - User can say anything, not bound by a grammar or a pre-defined pass phrase.
- Speaker Tracking

Appendix B - Continued on next page

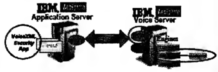
- Continuously monitor entire calls for assurance that the verified speaker answered all prompts.

- ♦ Speaker Change Detection
  - Can alert when a different speaker is detected in call (For example, a person calls in but then a friend takes over the conversation).

Your telephone self-service application can take advantage of this flexibility and provide a truly integrated and non-intrusive verification process. Since anything you say as part of a transaction dialog can be used to verify your identity, there is no need to remember pass-phrases or go through a separate verification process. For instance, you can prompt for an account number, have it recognized and the caller verified through the same dialog.

IBM has over 60 patents and 30 papers associated to its Speaker Verification technology, including a patent selected as one of Five Killer Patents by the MIT Technology Review Magazine (May/2004 issue).

IBM, via a services offering, provides a policy manager which complements the speaker *identity* verification feature of the WebSphere Voice Server. The policy manager adds a dynamic question and answer dialog to the caller interaction, further increasing security by validating customer specific information in combination with a voiceprint.



Use of Standards

IBM continues its commitment to standards with J2EE, MRCP, and the World Wide Web Consortium (W3C) Speech Interface Framework. The use of open standards has proven to be a driving force towards lowering solutions costs. This is particularly true in the speech, where applications are more and more based on a vast collection of industry standards.

IBM WebSphere Voice Server confirms IBM's commitment to support, adopt, and drive open standards. It ties together more than 35 years of worldwide speech research and technology expertise with the infrastructure provided by the IBM WebSphere platform.

Along with MRCP, WebSphere Voice Server supports the W3C Speech Interface Framework of standards, including voice grammars (SRGS), and speech markup (SSML).

Speaker *Identity* Verification for WebSphere Voice Server

WebSphere Voice Server builds on the base of the WebSphere Application Server to provide scaling, load balancing, failover, recovery, systems management, logging, tracing, and problem determination.

WebSphere Voice Server plays a major role as the foundation for IBM speech solutions. It provides a robust and scalable platform for speech functions like automated speech recognition and text to speech in addition to speaker identity verification.

For more information

This solution is available through IBM Software Services for WebSphere.

To learn more, contact your IBM representative or IBM Business Partner, or visit: ibm.com/speech

Exhibit C

customer care solutions
from Nuance

The experience speaks for itself

NUANCE

Nuance Verifier™ 4.0 :: Voice Authentication Software for Secure Access over the Telephone

Nuance Verifier 4.0, Nuance's advanced voice authentication software, enables businesses to provide secure access to sensitive information over the telephone. Like a fingerprint, Nuance Verifier voice authentication software creates individual voiceprints to authenticate callers and customers with just their voices, enabling secure access to information. Nuance Verifier 4.0 can also deliver improved caller satisfaction through convenient access to key automated speech solutions, including Financial & Retail transactions and account management, personal information access, time management, PIN reset, and benefit access. Adding voice authentication to these applications may result in increased use of automated systems and reduced fraud, saving Call Center costs. When deployed with Nuance speech recognition and text-to-speech, businesses around the world can build a range of secure, cost effective applications that can increase automation and improve customer satisfaction.

meeting the security challenge: voice authentication

Companies today have a wide range of options to choose from for security: touch-tone PINs, agent identification questions (e.g., "What are the last four digits of your social security number?"), pre-chosen passwords and now, voice authentication. Of those options, voice authentication offers the best combination of accuracy, convenience, and cost-effectiveness. This biometric technology captures specific physical characteristics of the human voice, using those characteristics to identify callers, something that other security measures just cannot do. This technology can also be a fundamental component of a multi-factor authentication approach. From securing financial transactions to allowing access to private health records, voice authentication takes security to a whole new level – with just a telephone and the human voice.

reduce the costs of customer service by increasing automation

Typically, security measures such as touch-tone PINs and agent questions have a high cost associated with them. PINs can be forgotten, so a customer service representative must reset them. After resetting the PIN, the representative may not be able to send the caller back to the automated system, requiring them to assist the caller with a transaction that a more cost-effective automated system could otherwise complete. In addition, agent identification questioning can take up to a minute to complete, increasing the overall length of an already long and expensive call.

Nuance Verifier 4.0 can reduce the costs associated with both of these security options. Customers may no longer need to remember long complicated PINs, reducing the costs associated with PIN resets. In addition, no longer needing to reset PINs could allow callers to remain in the automated system to complete their transactions. Using Nuance Verifier 4.0 to identify a caller prior to transferring the call to an agent can reduce the length of a call by removing the need to ask identifying questions. In addition, agents are freed up to handle more complex tasks rather than spending time identifying the caller.

consumers find voice authentication convenient and secure

A study by Touchpoint Consulting determined that consumers are comfortable using voice authentication as a means of convenient and secure access. In fact, 88% of participants found voice authentication to be more or equally convenient than touch-tone PINs. Seventy-four percent of participants also felt that voice authentication was more or equally secure than PINs.

using Nuance Verifier 4.0

Using Nuance Verifier 4.0 is simple. Callers participate in a brief, one-time enrollment process during which they answer several questions, allowing Nuance Verifier to capture and store their voiceprint. The voiceprint is not a recording, but an encrypted file similar to that found in fingerprinting technology. When a caller accesses the application at a later point, Nuance Verifier compares the caller's voice to the voiceprints on file. If Nuance Verifier finds a match, the caller gains access to the system.

state of the art technology

Nuance Verifier 4.0 builds upon years of Nuance research and deployment expertise to deliver high levels of accuracy and security to applications. It allows for a single voiceprint enrollment for ongoing use from any phone at any time, provides high accuracy for use in noisy, wireless and hands-free environments, and has the ability to adapt to changes in a caller's voice to ensure that applications using Nuance Verifier will be easy for callers to use over and over again. While results vary by application, Nuance Verifier 4.0 has achieved false accept rates lower than one percent.

maximum flexibility

Nuance Verifier 4.0 applications can be developed to meet a wide range of customer needs. Applications can be deployed with very high security for access to highly sensitive information such as financial or health care information. Nuance Verifier 4.0 can also support applications with convenience in mind, such as remote time management reporting. Companies have the flexibility to determine the best mix of security and convenience to meet their application needs. In addition, Nuance Verifier 4.0 provides options for enrollment and verification that allow groups to share the same identifier, enroll and verify using rotating questions, or even verify callers in the background while the callers are completing other tasks.

Nuance Verifier deployments made easier

Nuance enables partners and customers to reduce voice authentication application deployment time by up to 25% through tuning capabilities and mentoring services. Nuance Verifier 4.0 includes application logs that track key performance data, allowing for more effective application tuning and analysis. Nuance also offers Verifier Mentoring Services that provide partners and customers with mentoring on voice authentication application design, testing methodologies and tuning analysis. These services leverage Nuance's expertise in Nuance Verifier deployments and enable partners and customers to deploy effective applications to their customers, and ultimately, deliver satisfied callers.

supporting multi-factor authentication

Multi-factor authentication is becoming increasingly important as a defense to growing threats of security attacks, especially security attacks based on obtaining an individual's password via 'social engineering' (trickery). The 2005 FFIEC guidance, "Authentication in an Internet Banking Environment", and the follow-on FAQ in 2006 focus on further increasing the security of all electronic banking channels, including the telephone. The FFIEC recommends that financial institutions employ two of the following three factors to maximize security:

- Something the user possesses – (e.g., a token, ATM card, or USB device)
- Something the user knows – (e.g., a shared secret, password, or account number)
- Something the user is – (e.g., a fingerprint, iris scan or voice print)

Speaker verification solutions support a highly secure, cost effective approach to customer multi-factor authentication over the voice channel.

Nuance Verifier 4.0 offering

- Effective in a wide range of environments—landline, wireless or handsfree phones
- Language-independent, does not required speech recognition
- High accuracy
- One-time enrollment for verification during any subsequent call, from any type of phone
- Speaker identification allows multiple users to share an account or identifier
- Ongoing adaptation of voiceprint characteristics as voices change or age, improving the quality of voiceprints for faster, more accurate verification
- Supports liveness testing to safeguard against 'spoofing' with recorded speech
- Channel and gender identification
- Server architecture supports high transaction volumes
- Accessible via standard VXML
- Verification using letters, numbers, alphanumeric strings, phrases, etc.
- Dynamically detects if more information is needed to verify callers
- Advanced logging for more effective application tuning
- Can increase system automation and cost savings by reducing reliance on live agents to identify customers
- Can reduce occurrences of PIN resets, reducing call center costs
- Can increase security of information access, reducing the potential for fraud and identity theft
- Can improve customer service with a convenient means of security
- Flexible means of verification for individuals or groups
- Simple maintenance, load balancing and fault tolerance

operating systems

- Windows® Server 2003
- Red Hat Linux ES 4.0

about Nuance Communications

Nuance is the leading provider of speech and imaging solutions for businesses and consumers around the world. Its technologies, applications, and services make the user experience more compelling by transforming the way people interact with information and how they create, share, and use documents. Every day, millions of users and thousands of businesses experience Nuance's proven applications and professional services. For more information, please visit www.nuance.com.

NUANCE COMMUNICATIONS, INC. one wayside road burlington ma 01803 781 565 5000 nuance.com

Exhibit D

KIVOX

Your voice is the key

Data Sheet

KIVOX Verifier

Protect your systems against identity fraud using AGNITIO's voice biometrics technology

Secure Identity verification

KIVOX is AGNITIO's technology for strong speaker authentication solutions. It is the most reliable and robust voice biometrics engine available in today's market, with more than 15 years experience in the law enforcement sector and present in 22 countries.

KIVOX verifies a user's identity in a secure, user friendly, natural way, using common day to day devices such as a mobile phone and your own voice.

It is designed to be integrated in a wide variety of platforms and applications. KIVOX Verifier will help your organisation improve security, reduce cost and enhance user experience. Since voice biometrics is where security meets user convenience.

KIVOX verifier is based on free speech technology (text independent), so the user can be verified saying anything in any language. This technology is also channel independent (Landline, mobile, VOIP).

Applications

KIVOX Verifier can be easily integrated in any application that requires secure speaker verification.

KIVOX Verifier provides text independent voice biometrics technology. Therefore verifications can be performed in non-collaborative scenarios, or those that do not require the speaker to repeat a specific text.

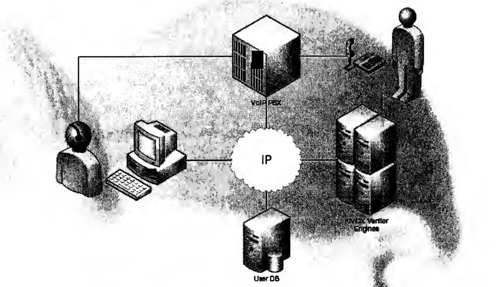
Some examples of KIVOX Verifier applications are:

- Multi-channel authentication for phone-banking & e-banking
- Private banking / Trade floor operations
- Background identity check
- Automatic conversation indexing per speaker
- Voice Signature
- Conference Call end-point authentication service.

About Agnitio

AGNITIO is the worldwide leader in voice biometrics in public security and has successfully adapted its robust technology for suitable corporate authentication solutions. AGNITIO's technology was first developed in the mid nineties. Today, AGNITIO's technology is deployed in over 22 countries for forensic applications of which the first renditions were co-developments with some of the world's most reputable police organizations. AGNITIO's KIVOX product provides the most advanced voice biometric solution to corporate organizations that is essential in offering end users an enhanced security solution. From an end user perspective voice biometrics provides a more user friendly and convenient solution that is time efficient.

Example of integration architecture



Feature	Kivox Verifier
Enrollment over landline telephone	✓
Enrollment over VoIP phone	✓
Verification over landline telephone	✓
Verification over VoIP phone	✓
Verification over Mobile phone	✓
Enrollment length	Configurable
Verification length	Configurable
Number of verification attempts	Configurable
Interfaces	C
Language Availability	Any
Signal Quality Check (SNR Check)	✓
Verification Grammar	Any
Verification Strategy	Free Speech
User ID used for verification	Optional
Verification time	Less than 0.15 seconds per net audio second
Supported OS	Windows XP, Vista, 2003 Server, 2008 Server

Hardware Requirements

Minimum configuration for running the API:

- Intel Core 2 Duo 2.4GHz or higher (3 GHz recommended)
- 1 GB RAM (4GB recommended)
- Network Card
- 300 MB HDD free space for setup data (1GB SCSI recommended)

AGNITIO

KIVOX

Your voice is the key

Exhibit E

Please see next page

Loquendo VoxNauta Platform

VoiceXML & CCXML PLATFORM

Loquendo VoxNauta platform enables carriers, enterprises, service providers and emerging technology companies to develop speech-enabled applications which follow the Web-based architecture enforced by VoiceXML and CCXML standards.

CCXML makes call control very flexible, while VoiceXML is focused on the voice interaction aspect of the application.

Loquendo VoxNauta can have Loquendo's ASR and TTS technologies optionally integrated - the most advanced speech technologies on the market today with complete support for all the relevant standards, and with many highly innovative features for an optimal exploitation of speech applications.

A Complete, Adaptable and Scalable Platform

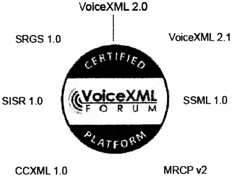
Loquendo VoxNauta SW platform has been further improved to allow efficiency, scalability and the best state-of-the-art performance for speech application development. The following are just a few features:

- VoxNauta platform's modular architecture makes it independent from Loquendo ASR/TTS engines and language/voice packages, allowing the **seamless upgrade** to new technology releases and new languages and voices.
- Speech technology ports are independent from the number of sessions running concurrently on the platform. This allows **cost savings** where ASR and TTS are only partially used, or not integrated.
- **VoxNauta is multi-OS**: both Windows and Linux operating systems are supported.
- Configuration, administration and management tasks are made easier by a simple but powerful **Graphic Management Console**.

Full Standard Compliance

Loquendo VoxNauta platform and Loquendo's speech technologies fully support all the most advanced IETF and W3C standards relevant to the voice market:

- Loquendo Voxnauta platform has been certified as **compliant with W3C VoiceXML 2.0 Recommendation** by the VoiceXML Forum Platform Certification program. In addition, all the **new features of VoiceXML 2.1** are also available.
- **Call Control is programmable** by means of **CCXML 1.0** scripts, the new powerful W3C standard complementing VoiceXML for call control handling. Simple actions, such as call initiation, conditional acceptance of a call, different kinds of call transfer, (up to the most complex call control features like conferencing, proactive outbound calls), are easily programmed by with this new markup language.



Standards and speech technologies:

- **Loquendo ASR** fully supports **SRGS 1.0** (Speech Recognition Grammar Specification), in both the XML and ABNF formats, for defining speech and DTMF grammars. Moreover, semantic interpretation fully implements the **SISR 1.0** (Semantic Interpretation for Speech Recognition) which allows a standard and powerful formatting of ASR results.
- **Loquendo TTS** fully implements **SSML 1.0** (Speech Synthesis Markup Language) offering standard controls to enhance TTS rendering, thus achieving the best experience for the user. All the unique features offered by Loquendo TTS are also accessible in SSML.
- **Uniform ASR and TTS user lexicons** are offered to the VUI developer, and the standardization of **PLS 1.0** (Pronunciation Lexicon Specification) is a primary goal to ensure a fully standards compliant application development.

www.loquendo.com

Loquendo

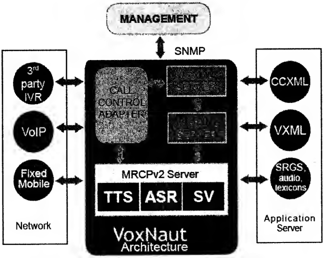
Current Set-up

Loquendo VoxNauta platform is typically applied in the world of telephony, e.g. in IVRs, speech-enabled self-service applications, etc. It is standards-based, so that even a DTMF based application can be programmed in VoiceXML/CCXML, and subsequently "upgraded" to voice-interaction leveraging optional speech technologies. VoxNauta can be used on both **VoIP** (SW-only SIP/RTP implementation) and **TDM** networks (through VoIP-TDM Gateways or third-party telephony cards).

New scenarios are also emerging which can benefit from the flexibility of VoxNauta platform, such as the delivery of **voice and video applications** (multimedia) for advanced mobile and video telephony applications, as well as **multimodal applications** based on embedded TTS and DSR.

CCXML call control

The W3C's new markup language, **CCXML** (Call Control XML) is used to define the call control part of telephony applications. CCXML is an event-driven markup language which is able to efficiently dispatch telephony events and launch VoiceXML applications. Its key design features of CCXML are its **ease of use**, **flexibility**, and ability to deal with **complex applications**.



CCXML Highlights

- *Asynchronous event processing*
- *Conditional acceptance or refusal of incoming calls*
- *Several kinds of call transfer*
- *Outbound call initiation*
- *Scripting capabilities (ECMA-327)*
- *VoiceXML management*
- *Conferencing management*

Flexible Call Control Services

CCXML applications range from simple ones such as playing an announcement on an incoming call or redirecting a call if certain conditions are met, to more complex ones such as the flexible description of a Conferencing system driven by a web application.

CCXML makes it possible to send and receive commands through an HTTP interface, making it easy to realize new interactive call control capabilities.

Moreover CCXML can handle VoiceXML dialogs for self-service applications and transfer a call back and forth to an operator. The flexibility of CCXML allows call initiation driven by events from an application server. The VoxNauta platform implements version 1.0 of the CCXML draft standard of W3C.

VoiceXML applications

VoiceXML is now acknowledged by an ever-increasing number of speech-application developers as a must for all telephony platforms, and together with CCXML is a key feature of the Loquendo VoxNauta platform.

VoiceXML 2.1 Extensions

VoiceXML 2.0 is now widespread and its compliance enforced by the **VoiceXML Forum Platform Certification program** (www.voicexml.org). New features have been recently added, to produce VoiceXML 2.1.

The major VoiceXML 2.1 features are:

- ***Audio recording during speech recognition*** *- a key feature for call logging, data mining and speech application tuning. It also allows external speech engines to detect innovative features during the course of a speech interaction.*
- ***A new <data> element*** *fetches XML data during the processing of a VoiceXML page. This allows the adaption of the VoiceXML dialog strategy according to external XML data, without the need to edit the VoiceXML page. One very important use is the fetching of a dynamic list of prompts that are specific to the speech interaction, e.g. a list of movies in a cinema.*
- ***A <foreach> element*** *process a dynamic list of prompts.*
- ***A new type of transfer call,*** *called "consultation", has been added to "blind" and "bridge" types. It allows a call transfer to be attempted and, in the case of no reply or an error, returns to the speech application to continue the dialog.*

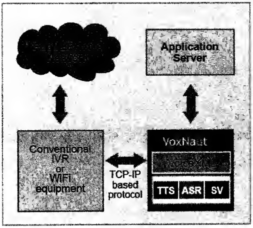
The VoxNauta platform implements all the VoiceXML 2.1 features to extend the flexibility and power of VoiceXML applications.

Web based applications

With the adoption of VoiceXML and CCXML, all applications and application content can be dynamically fetched from a Web server. This is also true for SRGS grammars, user lexicons, audio prompts and music. It greatly simplifies application development and allows a complete, clear separation of the application layer from the media and management layer.

Loquendo VoxNauta

Innovative Application Scenarios



Network Integration Capabilities

Besides conventional network interfaces, VoxNauta offers a TCP/IP-based application layer protocol interface (DAP). This allows for the **upgrade of any conventional IVR platform**, or any other private network interfacing equipment (e.g. WiFi), with the new and essential features offered by VoiceXML 2.0 and 2.1. At the same time, it exploits optimal integration with Loquendo speech technologies (Loquendo TTS and Loquendo ASR).

In short, any third party equipment can still leverage its own call control mechanism or access techniques, while **upgrading to a fully standards compliant VoiceXML** platform.

The integration, which leverages a simple message-based protocol, **is straightforward**, saves time and outlay for companies wishing to exploit a certified VoiceXML browser without having to worry about technology integration.

O&M integration is also ensured by the **SNMP** interface available with VoxNauta

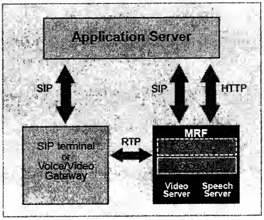
Multimedia Capabilities Toward IMS

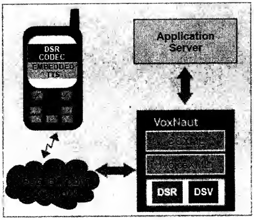
The aim of 3GPP (UMTS scenario), to ensure convergence of cellular and internet technologies, has led to the standardization of the **IP Multimedia Subsystem (IMS) architecture**, in which multimedia applications are hosted on a SIP application server, described in CCXML and VoiceXML and executed by an MRF (Media Resource Function) component.

Therefore, the *essential elements* of an MRF are the **CCXML interpreter**, the **VoiceXML interpreter**, the **speech server** for TTS, ASR and DTMF management and the **video server** for streaming, video/image presentation and co-decoding.

Both CCXML and VoiceXML are **media agnostic** and therefore suited both for speech and video application development.

Moreover, with the introduction of a few specific, **additional VoiceXML elements** for video/image presentation and push-to-talk options, VoxNauta is at the forefront for this new emerging and challenging market opportunity.





Multimodal Capabilities over Mobile Data Networks

Loquendo VoxNauta platform can also be used as a **network server in multimodal application** development for mobile data networks (e.g. GPRS), by exploiting the capabilities of DSR (Distributed Speech Recognition) encoding and Loquendo Embedded TTS.

In this context, multimodal applications are activated by a thin client on the mobile phone, and described in VoiceXML/CCXML as any other vocal applications.

Uplink payload for **vocal commands** is dramatically reduced by **DSR encoding** of the speech front-end parameters, which also ensures reduced channel errors' sensitivity.

Downlink payload is minimized by exploiting the **Loquendo Embedded TTS capabilities**, which can be installed on the terminal together with the client software.

In this way, developing multimodal services becomes as easy as writing VoiceXML applications.

Loquendo VoxNauta

Infinite Solutions for All IVR and Self-Service Applications

VoxNauta is designed for the development of any kind of IVR and speech-enabled, self-service application, including:

- **Information services** - to access information on services and products, customer service and public information such as opening hours and office locations;
- **Personal communication services** - using a personal/ business profile to access a personal address book, e-mail by phone, agenda and calendar applications;
- **Transactional services** like online trading, home banking, travel booking, voice-commerce or insurance services etc.

Loquendo VoxNauta - Technical Specifications

System Configurations	**IVR:** includes CCXML, VoiceXML, DTMF and prerecorded audio **ASR only:** includes CCXML, VoiceXML, DTMF, ASR and prerecorded audio **TTS only:** includes CCXML, VoiceXML , DTMF, prerecorded audio and TTS **Full dialog advanced IVR:** includes CCXML, VoiceXML, DTMF, ASR, SV, prerecorded audio and TTS
OS Supported	Microsoft Windows (Server 2003 English Edition, Server 2008 English Edition), Red Hat Enterprise Linux (4.0, 5.1)
Network Signalling (TDM)	Analog (Loop Start), Euro-ISDN
Supported Telephone Cards	NMS AG 2000/200-8LSE (Analog), NMS AG4000/400-1E (Euro-ISDN), NMS AG4040/4-1TE (Euro-ISDN), Intel Dialogic DMV600BTEP (Digital), NMS CG6565 (Euro-ISDN)
Echo Cancellation	Supported by telephone cards
Network Signalling (VoIP: SIP-RTP)	RFC 3261 (Session Initiation Protocol), RFC 3515 (Refer Method), RFC 2327 and 3264 (SDP) RFC 3891 (Replaces Header), RFC 1889 (RTP), RFC 3665 (Basic Call Flow), RFC 3666 (PSTN Call Flow), RFC 2833 (DTMF), RFC 4240 (Netann)
Speech Related Standards	CCXML 1.0, VoiceXML 2.0, VoiceXML 2.1, SRGS 1.0 (XML and ABNF), SISR 1.0, SSML 1.0, DSR Aurora, HTTP/HTTPS 1.1
File Fetch	CCXML and VoiceXML documents, as well as SRGS grammars, lexicon and audio files are fetched from local file system and over HTTP (with caching support) and/or HTTPS
Voice Coding	G.711 (A-law and µ-law)
Audio File Formats	8 and 16 bit, A-law, µ-law and linear, mono, 8 kHz
Speech Technologies	Loquendo ASR, Loquendo SV, Loquendo TTS (via MRCPv2)
Supported Languages	American English, Canadian French, Brazilian Portuguese, American Spanish, Argentinian Spanish, Chilean Spanish, Mexican Spanish, British English, Castilian Spanish, Catalan, Valencian, Galician, Dutch, French, German, Greek, Italian, Polish, Portuguese, Swedish, Turkish, Arabian, Russian, Finnish, Danish and Mandarin Chinese
O&M	SNMP and Graphic Centralized Management Console
System Profiles	VoIP (SIP/RTP), TDM network (with NMS card), TDM network (with Dialogic card), DAP* (TCP-IP interface).

* DAP profile does not include CCXML interpreter

For more detailed information see the **Loquendo TTS** and **Loquendo ASR** brochures
To find out how Loquendo's products can position your company for success, please visit **www.loquendo.com**

Loquendo - Vocal Technology and Services
Via Arrigo Olivetti, 6 - 10148 Torino - Italy
tel. +39 011 2913111 - fax +39 011 2913199
www.loquendo.com info@loquendo.com

Loquendo
VOCAL TECHNOLOGY AND SERVICES

LOQ-FEB 2009

Exhibit F

Leave impersonators, fraudsters and identity thieves speechless.

VocalPassword™ 6.0

Reduce fraud with text-dependent speaker verification that is secure, convenient and cost effective.

Escalating incidents of identity theft, fraud and social engineering attacks continue to compromise existing data security measures. Traditional single-factor authentication approaches including passwords and challenge questions no longer provide the necessary safeguards for secure remote services. Biometric speaker verification technology uses the power of voice to provide the critical component in an effective multi-factor authentication solution.

VocalPassword is a unique text-dependent biometric speaker verification system that enables verification and identification of a speaker in real time, using a simple spoken pass phrase. Totally language and accent independent, VocalPassword provides a secure, efficient and extremely convenient method to verify a speaker's identity.

VocalPassword is easy to deploy, seamlessly integrating with existing IVR and VoiceXML platforms. Designed exclusively to meet strict global security standards, VocalPassword has successfully passed independent security audits. Featuring state-of-the-art accuracy, VocalPassword is used to secure access to remote services, telephony and Web applications, effectively combating identity fraud and enhancing the customer experience.

VocalPassword has been selected as the speaker verification platform of choice by leading financial services, telecom operators and security organizations, as well as IVR/voice platform vendors and system integrators worldwide.

Features
- Language and accent independent
- State-of-the-art accuracy
- Straightforward deployment
- Integrated security
- Convenient and non-intrusive (no personal information required)
- Secure multi-factor authentication

Benefits
- Reduced call duration in call centers
- Secured transactions
- Enhanced customer experience

Applications
- Secure access for remote services/transactions (phone and Web)
- Contact center/helpdesk interactions
- Automated self-service
- Password reset
- Secure conferencing
- Offender monitoring
- Remote time and attendance

Markets
- Financial Services
- Enterprise Security
- Government and Law Enforcement
- Telecommunications
- Insurance
- Healthcare

GLOBAL SUPPORT
PerSay maintains an extensive network of partners and system integrators, including IBM and British Telecom. The company has over 60 installations worldwide and provides local support in more than 20 countries, including the U.S., Canada, Spain, Sweden, Turkey, China, Korea, South Africa, Brazil, Colombia and Australia.

Advanced Biometric Speaker Verification

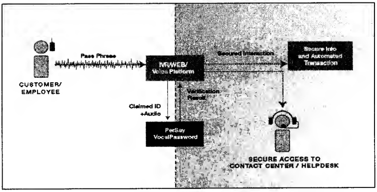
PerSay™
Voice Biometrics

How It Works

VocalPassword interacts with IVRs. Web servers and voice platforms to provide secure access to contact centers and private and sensitive information. The speaker's pass phrase, acquired by the IVR/Web server, is transferred to VocalPassword along with a claimed identity. A verification result is then returned by the system to the IVR\Web server confirming the speaker's identity.

Enrollment
Enrollment in VocalPassword is carried out by three consecutive renderings of the selected pass phrase, creating a unique voiceprint.

Verification
VocalPassword verifies the speaker by comparing a single repetition of the enrolled pass phrase to the voiceprint stored in the system's voiceprint repository.



About PerSay
PerSay Ltd (www.persay.com) is a leading provider of advanced biometric speaker verification products. PerSay's technology relies on the biometric power of voice to verify a speaker's identity. PerSay's products have been deployed by leading financial services, telecom operators, healthcare providers, enterprises and law enforcement agencies worldwide. PerSay is a spin-off of Verint Systems Inc., with offices in Tel Aviv and New York, and a network of partners and system integrators worldwide.

PerSay™
Voice Biometrics

Exhibit G

SpeechSecure from SpeechWorks

Speaker verification technology conveniently enhances caller security

SpeechWorks' SpeechSecure™ uses biometric technology to verify a caller's identity based on the characteristics of his or her unique vocal patterns. SpeechSecure provides a convenient and extremely tight level of security for callers who access personal information over the telephone. From financial services to telephony services, SpeechSecure opens the door to a host of commercial applications where high security and/or high convenience is required.

Customer Benefits

Caller convenience: Used in combination with automated speech recognition, SpeechSecure recognizes and verifies a caller as an ID or account number is spoken, eliminating the need to remember and enter a password.

Enhanced security: When combined with a password, SpeechSecure adds another level of security, confirming that the right person said the right password.

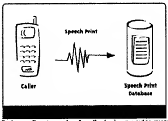
Lower costs: Call center services such as caller verification or PIN reset that previously required customer service representative interaction (and associated 800-toll costs while on hold) can now be offered using automated speech recognition applications and speaker verification, freeing up customer service representatives to focus on more value-added activities.

Differentiation: SpeechSecure allows companies to maximize the impact and business reach of their speech solution portfolio.

How it Works

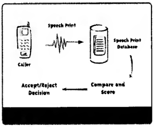
Speaker verification occurs in two phases, enrollment and verification.

Enrollment: New callers are prompted to say their passwords three times; these recordings are used to create a reference "speech print".



During enrollment, samples of a callers' voice are used to create a reference speech print which is stored in a database.

Verification: Whenever a person calls and attempts to access an account, the caller's speech print is compared with the reference speech print for that account. A resulting confidence score is compared against security thresholds to determine whether the caller is granted access.



During verification, the callers' speech print is compared with the reference speech print to verify authenticity.

SpeechSecure Features

Plug & Play architecture: SpeechSecure can be easily integrated into a SpeechWorks® speech application (version 6.5 or later).

Language-independent: Allows the caller to select any word or phrase – in any language – as a password.

Verification options: SpeechSecure includes two DialogModules™, both of which provide high accuracy and virtually eliminate the possibility that an imposter will access a caller's account by imitating the caller's voice.

- The Verification DialogModule enrolls and verifies a password phrase speech print.
- The Digits Verification DialogModule includes the ability to recognize a digit string (e.g., account number) and verify the speech print simultaneously.

Security vs. flexibility: Verification parameters can be tuned to achieve the desired balance between high security (minimizing "False Acceptances" or allowing imposters in) and flexibility (minimizing "False Rejections" or keeping out legitimate users).

Verification robustness: SpeechSecure can isolate the password from extraneous sounds (e.g., cellular artifacts, clicks, stutters, background noise, etc.), resulting in higher accuracy.

Smarter speech prints: With additional calls and samples of the caller saying a password, the speech print can be updated to provide a more characteristic model of the caller's voice, thereby ensuring that authentic callers can access their accounts, while preventing access to unauthorized callers.

Installation and Configuration

SpeechSecure: SpeechSecure is packaged on a CD as a DialogModule which includes the verification engine, sample applications, the feature sets database and speech print update tool.

Voice model database: Speech prints are stored in a database that is implemented using Microsoft SQL Server 7.0. Alternatively, ODBC (open database connectivity) is used with SpeechSecure to allow other databases to be used instead of SQL server.

SpeechWorks, Partner of Choice

A global company, SpeechWorks provides products and services to leading companies worldwide that want to offer superior, cost-effective customer service using speech solutions. The partner of choice, SpeechWorks delivers award-winning, cutting-edge technology, and is committed to open standards in the development of speech services. SpeechWorks offers results-assurance programs including the SpeechWorks Here™ Guarantee and Market Accelerator Program, and ROI accelerator solutions such as the SpeechSpot™. SpeechWorks' professional services group, one of the largest in the world for the development of speech applications, is known in the industry for its market-proven process and dedication to customer satisfaction.

SpeechWorks

For more information:

SpeechWorks International, Inc.
695 Atlantic Avenue
Boston, MA 02111

Tel: +1.617.428.4444
Fax: +1.617.428.1122
Email: info@speechworks.com
Demo: 1.888.SAY.DEMO
www.speechworks.com